Qualys. SSL Labs

Home Projects Qualys.com Contact

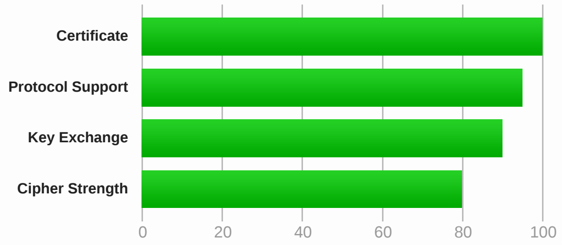
**You are here:** Home > Projects > SSL Server Test > flow-wolf.org > 2a05:d01c:812:a200:9de0:f77:e347:57d2

# SSL Report: flow-wolf.org (2a05:d01c:812:a200:9de0:f77:e347:57d2)

## Summary

Overall Rating

A+



**Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.**

**HTTP Strict Transport Security (HSTS) with long duration deployed on this server.** MORE INFO »

## Certificate #1: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | flow-wolf.org<br>Fingerprint SHA256: e3ea5d7a5c499f03683d739e20025afe2a6e622211c6ccd44705187faeda80c4<br>Pin SHA256: E7IEvVUQ0QQtJr9sllZaPDiQ0U6mUgpDqVjsERMEhn0= |
| **Common names** | flow-wolf.org |
| **Alternative names** | flow-wolf.org |
| **Serial Number** | 030821dbc16558f416cfc361f3461347a43c |
| **Valid from** | Mon, 13 Nov 2017 21:37:20 UTC |
| **Valid until** | Sun, 11 Feb 2018 21:37:20 UTC (expires in 2 months and 28 days) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | Let's Encrypt Authority X3<br>AIA: http://cert.int-x3.letsencrypt.org/ |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | No |
| **OCSP Must Staple** | No |
| **Revocation information** | OCSP<br>OCSP: http://ocsp.int-x3.letsencrypt.org |
| **Revocation status** | Good (not revoked) |
| **DNS CAA** | No (more info) |
| **Trusted** | **Yes** |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 2 (2455 bytes) |
| **Chain issues** | None |

**#2**

| | |
|---|---|
| **Subject** | Let's Encrypt Authority X3<br>Fingerprint SHA256: 25847d668eb4f04fdd40b12b6b0740c567da7d024308eb6c2c96fe41d9de218d<br>Pin SHA256: YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg= |
| **Valid until** | Wed, 17 Mar 2021 16:40:46 UTC (expires in 3 years and 4 months) |

### Additional Certificates (if supplied)

| | |
|---|---|
| Key | RSA 2048 bits (e 65537) |
| Issuer | DST Root CA X3 |
| Signature algorithm | SHA256withRSA |

### Certification Paths

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | No |
| SSL 2 | No |

For TLS 1.3 tests, we currently support draft version 18.

### Cipher Suites

#### # TLS 1.2 (suites in server-preferred order)

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS | 128 |

#### # TLS 1.1 (we could not determine if the server has a preference)

#### # TLS 1.0 (we could not determine if the server has a preference)

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Chrome 57 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Firefox 53 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Googlebot Feb 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| IE 7 / Vista | Server sent fatal alert: handshake_failure | | |
| IE 8 / XP No FS [1] No SNI [2] | Server sent fatal alert: handshake_failure | | |
| IE 8-10 / Win 7 R | Server sent fatal alert: handshake_failure | | |
| IE 11 / Win 7 R | Server sent fatal alert: handshake_failure | | |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 2048 FS |

### Handshake Simulation

| | | | | |
|---|---|---|---|---|
| IE 10 / Win Phone 8.0 | Server sent fatal alert: handshake_failure | | | |
| IE 11 / Win Phone 8.1 R | Server sent fatal alert: handshake_failure | | | |
| IE 11 / Win Phone 8.1 Update R | Server sent fatal alert: handshake_failure | | | |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Edge 13 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Java 6u45 No SNI [2] | Client does not support DH parameters > 1024 bits<br>RSA 2048 (SHA256) \| TLS 1.0 \| TLS_DHE_RSA_WITH_AES_128_CBC_SHA \| DH 2048 | | | |
| Java 7u25 | Client does not support DH parameters > 1024 bits<br>RSA 2048 (SHA256) \| TLS 1.0 \| TLS_DHE_RSA_WITH_AES_128_CBC_SHA \| DH 2048 | | | |
| Java 8u31 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| OpenSSL 1.0.2e R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DH 2048 FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 > http/1.1 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 FS |

#### # Not simulated clients (Protocol mismatch)

| | |
|---|---|
| IE 6 / XP No FS [1] No SNI [2] | Protocol mismatch (not simulated) |

**(1) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.**

(2) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(3) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(4) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

### Protocol Details

| | |
|---|---|
| **DROWN** | No, server keys and hostname not seen elsewhere with SSLv2<br>**(1) For a better understanding of this test, please read this longer explanation**<br>(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here<br>(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete |
| **Secure Renegotiation** | **Supported** |
| **Secure Client-Initiated Renegotiation** | No |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: 0x33 |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | No (more info) |
| **Downgrade attack prevention** | **Yes, TLS_FALLBACK_SCSV supported** (more info) |
| **SSL/TLS compression** | No |
| **RC4** | No |
| **Heartbeat (extension)** | Yes |
| **Heartbleed (vulnerability)** | No (more info) |
| **Ticketbleed (vulnerability)** | No (more info) |
| **OpenSSL CCS vuln. (CVE-2014-0224)** | No (more info) |
| **OpenSSL Padding Oracle vuln. (CVE-2016-2107)** | No (more info) |

### Protocol Details

| | |
|---|---|
| Forward Secrecy | Yes (with most browsers) ROBUST (more info) |
| ALPN | Yes http/1.1 |
| NPN | Yes http/1.1 |
| Session resumption (caching) | No (IDs assigned but not accepted) |
| Session resumption (tickets) | Yes |
| OCSP stapling | No |
| Strict Transport Security (HSTS) | Yes<br>max-age=31536000; includeSubDomains |
| HSTS Preloading | Not in: Chrome Edge Firefox IE |
| Public Key Pinning (HPKP) | No (more info) |
| Public Key Pinning Report-Only | No |
| Public Key Pinning (Static) | No (more info) |
| Long handshake intolerance | No |
| TLS extension intolerance | No |
| TLS version intolerance | No |
| Incorrect SNI alerts | No |
| Uses common DH primes | No |
| DH public server param (Ys) reuse | No |
| ECDH public server param reuse | No |
| Supported Named Groups | secp256r1 |
| SSL 2 handshake compatibility | Yes |

### HTTP Requests

1 https://flow-wolf.org/ (HTTP/1.1 200 OK)

### Miscellaneous

| | |
|---|---|
| Test date | Tue, 14 Nov 2017 21:15:32 UTC |
| Test duration | 82.125 seconds |
| HTTP status code | 200 |
| HTTP server signature | nginx/1.10.3 (Ubuntu) |
| Server hostname | - |

SSL Report v1.29.7

Terms and Conditions

Qualys is the leading provider of integrated infrastructure security, cloud infrastructure security, endpoint security, devsecops, compliance and web app security solutions.